SECURITY AND CRYPTOGRAPHY LABORATORY

Family Name: ....

First Name: ....

Section: ....

Security and Cryptography

Fall semester 2007

Midterm Exam
Solution

November 1st, 2007

Duration: 105 minutes

Part 1 / 2

This document consists of 8 pages.

Instructions

Documents are *not* allowed apart from linguistic dictionaries.

Electronic devices are *not* allowed.

Answers must be written on the exercises sheet.

This exam contains 2 *independent* exercises.

Answers can be either in French or English.

Questions of any kind will certainly *not* be answered. Potential errors in these sheets are part of the exam.

You have to put your full name on the first page and have all pages *stapled*.

1 Attacks on a Simple Cipher

Let $C : \{0,1\}^n \times \{0,1\}^m \mapsto \{0,1\}^n$ be a n-bit block cipher with m-bit keys. C consists of 2 rounds of a Feistel scheme as depicted on Figure 1. The plaintext is denoted by $x \in \{0,1\}^n$ and the output ciphertext by $y \in \{0,1\}^n$.

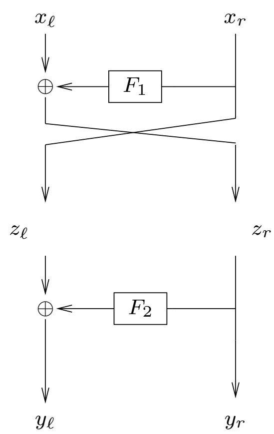
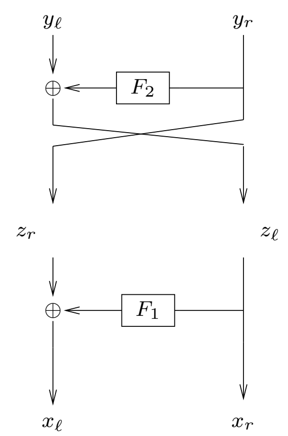


Figure 1: C: a 2-round Feistel scheme.

We use the notation $x_\ell, x_r \in \{0,1\}^{\frac{n}{2}}$ (resp. $y_\ell, y_r \in \{0,1\}^{\frac{n}{2}}$) for the plaintext (resp. ciphertext) on the left and right leaves, i.e., $x = x_\ell \| x_r$ and $y = y_\ell \| y_r$ where the operator "$\|$" denotes the concatenation.

1. Draw the inverse scheme for the Feistel scheme of Figure 1.



Now, we will define the round functions. Let the key $k \in \{0,1\}^n$, i.e. here $m = n$, and let $k_1, k_2 \in \{0,1\}^{\frac{n}{2}}$ be respectively the left and right part of k. We consider that the round function F_i with input α simply "xor" the input with the round key k_i, i.e. the output is

$$\beta = F_i(\alpha) = \alpha \oplus k_i.$$

2. Write y_ℓ and y_r in terms of x_ℓ, x_r, k_1, k_2.

First note that

$$z_\ell = x_r$$

and

$$z_r = x_\ell \oplus F_1(x_r) = x_\ell \oplus x_r \oplus k_1.$$

Then, we can write

$$\begin{aligned} y_\ell &= z_\ell \oplus F_2(z_r) \\ &= x_r \oplus (x_\ell \oplus x_r \oplus k_1) \oplus k_2 \\ &= x_\ell \oplus k_1 \oplus k_2 \end{aligned} \tag{1}$$

and

$$\begin{aligned} y_r &= z_r \\ &= x_\ell \oplus x_r \oplus k_1. \end{aligned} \tag{2}$$

3. Explain how it is possible to recover the key K using one plaintext-attack query, i.e. based on a plaintext-ciphertext pair (x, y).

If we know a pair (x, y), from Eq. (2), we deduce

$$k_1 = x_\ell \oplus x_r \oplus y_r \tag{3}$$

and from Eq. (1), we deduce

$$\begin{aligned} k_2 &= x_\ell \oplus y_\ell \oplus k_1 \\ &= x_r \oplus y_\ell \oplus y_r \end{aligned} \tag{4}$$

were we used Eq. (3) in the last equality.

Now, we build the cipher $2C$ by concatenating two times C as decpited on Figure 2.

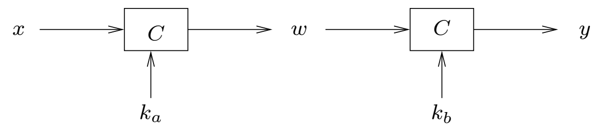


Figure 2: $2C$.

4. Considering C as a black-box, which well-known attack can be applied?

> Simply use a meet-in-the middle attack.

5. Write y_ℓ and y_r in terms of $x_\ell, x_r, k_{a1}, k_{a2}, k_{b1}, k_{b2}$.

> For the first C (with key $k_a = k_{a1} \| k_{a2}$), from Eq. (1) and (2), we directly find
>
> $$\begin{aligned} w_\ell &= x_\ell \oplus k_{a1} \oplus k_{a2} \\ w_r &= x_\ell \oplus x_r \oplus k_{a1}. \end{aligned}$$
>
> We can write the same for the second C (with key $k_b = k_{b1} \| k_{b2}$):
>
> $$\begin{aligned} y_\ell &= w_\ell \oplus k_{b1} \oplus k_{b2} \\ y_r &= w_\ell \oplus w_r \oplus k_{b1}. \end{aligned}$$
>
> Finally we substitute the w_i of the two first equations in the two seconds and we find :
>
> $$y_\ell = x_\ell \oplus k_{a1} \oplus k_{a2} \oplus k_{b1} \oplus k_{b2} \quad (5)$$
> $$y_r = x_r \oplus k_{a2} \oplus k_{b1}. \quad (6)$$

6. Is a decryption attack know possible? Explain your answer.

From last question, we note that

$$\begin{aligned} y_\ell &= x_\ell \oplus K_\ell \\ y_r &= x_r \oplus K_r \end{aligned}$$

were K_ℓ and K_r are constants (for a given key k_a, k_b)
So, just knowing a pair (x_0, y_0) allows to recover any message x_i given its ciphertext y_i by computing $x_i = y_i \oplus y_0 \oplus x_0$.
In conclusion, a decryption attack is possible only knowing a plaintext/ciphertext pair (x, y). Note that a key recovery attack is impossible.

7. Let y and y' be two ciphertexts. What can we say about $y \oplus y'$? What is the consequence?

We see that $y \oplus y' = x \oplus x'$ (from two last questions). So, given two ciphertexts, we can deduce information on plaintexts.

2 Linear Algebra

1. Compute $17^{129} \bmod 19$.
   Give the details.

First, we note that we are working in $\mathbb{Z}_{19}^*$. So, the group order is $\varphi(19) = 18$.
We can write

$$17^{129} = 17^{7 \cdot 18 + 3} \equiv 17^3 \pmod{19}$$

Then we do two iterations of the square-and-multiply algorithm, i.e.

$$17^3 = 17^2 \cdot 17 \equiv 4 \cdot 17 \equiv 11 \pmod{19}.$$

Otherwise, you can see that $17 \equiv -2 \pmod{19}$ and then

$$17^3 \equiv (-2)^3 \equiv -8 \equiv 19 - 8 \equiv 11 \pmod{19}.$$

2. Compute the inverse of 7 in $\mathbb{Z}_{143}^*$, i.e. compute $7^{-1} \bmod 143$.
Give the details.

Here, one solution is to use the Extended Euclid Algorithm as follows :

#			q
0	(143,0,1)	(7,1,0)	20
1	(7,1,0)	(3,-20,1)	2
2	(3,-20,1)	(1,41,-2)	3
3	(1,41,-2)	(0,-143,7)	

where the last row means that

$$1 = 41 \cdot 7 - 2 \cdot 143$$

which is in fact the Bezout identity.
So, the inverse of 7 $\pmod{143}$ is 41, i.e. $7^{-1} \equiv 41 \pmod{143}$.

**Any attempt to look at
the content of these pages
before the signal
will be severly punished.**

Please be patient.